REMARKS

Applicants are amending the specification to correct minor typographical errors. Thus, Applicants are adding no new matter to the specification. Furthermore, Applicants are amending the claims to cancel claims 1-4 and add new claims 5-40.

Applicants submit that the pending claims are in condition for allowance. Therefore, Applicants respectfully request entry of the preliminary amendment and early allowance of the claims.

Respectfully submitted,
JOHN S. FLOWERS *et al.*

Date: November 26, 2002

By: _____
Brian M. Hoffman, Reg. No. 39,713
Attorney for Applicants
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, CA 94306
Tel.: (415) 875-2484
Fax: (415) 281-1350

VERSION OF SPECIFICATION WITH MARKINGS TO SHOW CHANGES

Paragraph No. 1:

[0001] This application claims the benefit of U.S. Provisional Application No. 60/175,332, filed January 10, 2000, which is [and] incorporated herein by reference.

Paragraph No. 7:

[0007] To further burden the security engineer, each vulnerability or potential intrusion needs to be identified and a description of it stored for use by the vulnerability or intrusion detection tools. This process, however, is often complicated. For instance, it is extremely difficult just to write an application that would check a Secure Shell (SSH) server to determine if the remote system was running a version of SSH that is vulnerable to a Denial of Service attack. Traditional development methodologies force the user to have an intimate understanding of TCP/IP and a low-level (often cumbersome) development language such as ANSI C or Perl. Even advanced "Attack Scripting Languages" are overly cumbersome and require an understanding of variables, "for" loops, "while" loops, and other development syntax.

Paragraph No. 11:

[0011] An IDS used with an embodiment of the invention monitors network traffic for signs of malicious activity. This analysis of network traffic is also based on a set of rules. However, the rules used by the IDS are determined based on the analysis of the network performed by the VDS – the IDS only monitors for intrusive traffic that can actually affect [offset] the particular network.

Paragraph No. 26:

[0026] The rules referred to above that are stored in the rules database or loaded into the IDS are query-based, and resemble "assertions" or "queries" found in typical SQL. The rules are structured to be assertions that, if found true, identify the presence of a particular condition, such as an operating system, application, vulnerability, or intrusion. Hence, collectively, these rules serve to identify and name the characteristics and properties of the [a] network 100. For instance, to test for a vulnerability in the Line Printer Daemon (LPD) that shipped with the Solaris (Trademark of Sun Microsystems) operating system, the following conditions must be checked: (1) the scanned server is running the Solaris operating system, and (2) the scanned server is running LPD. Thus, the rules are constructed to define a vulnerability if these two conditions are present.